Ethical hacking lab : Toolbox HackTheBox

"Mi intención, además de llevar un Conteo y Evidencia de mi progreso en la formación como Pentester, es despertar la curiosidad en la comunidad mexicana y de habla hispana sobre temas de Hacking Ético. Quiero ofrecer lo que considero una explicación 'sencilla' de lo complejo y fascinante que son los sistemas vulnerables en la actualidad."

/▲\ Correo /▲\ tiktok /▲\ github

Atacante ---------- |10.10.19.30|

|>/////////// Linux|

Victima ---------- |10.10.11.130|

|> /////// Windows|

Walkthrough

| 1 | Enumeración de Servicios y Descubrimiento de Vulnerabilidades

Durante la enumeración de puertos y servicios, se identificó un servicio FTP con la credencial anonymous como válida, permitiendo el acceso al archivo "docker-toolbox.exe". Además, se detectó un servicio web activo asociado al subdominio admin.megalogistic.com. Este subdominio alberga un panel de autenticación vulnerable a inyección SQL, evidenciado por un error de sintaxis al probar la combinación ' AND ', que reveló información sensible del sistema dando PostgreSQL como su tecnología para su BD. Este comportamiento es una clara señal de vulnerabilidad, ya que este tipo de error no debería ser visible para el usuario.

| 2 | Explotación de la Inyección SQL para Lograr RCE

Investigando en HackTricks, se descubrió que es posible aprovechar esta inyección SQL para ejecutar comandos en el sistema mediante la creación de una tabla especial. Esta vulnerabilidad transforma la inyección SQL en un RCE (Remote Code Execution). Utilizando esta técnica, se logró establecer una conexión inversa (reverse shell) con el equipo víctima, ejecutando un script en bash mediante el comando curl | bash. Al enumerar las interfaces de red, se observó que la IP del sistema era 172.17.0.2, lo que sugiere que estábamos dentro de un contenedor Docker. Esta suposición, junto con el archivo compartido por FTP, fue suficiente para probar las contraseñas por defecto de Docker Toolbox, las cuales resultaron ser correctas. Esto nos permitió acceder a la primera flag de usuario y, debido a una mala administración de volúmenes, se obtuvo acceso al directorio .ssh, robando la clave pública del usuario Administrator.

| 3 | Pivoting y Escalada de Privilegios

Con la clave pública obtenida, se realizó un pivoting a la interfaz real del sistema con los máximos privilegios, lo que permitió un control total sobre el equipo comprometido.

Habilidades.

>- PostgreSQL Injection (RCE)

Una **inyección SQL** en PostgreSQL ocurre cuando un atacante manipula una consulta SQL al ingresar datos maliciosos en los campos de entrada de una aplicación web. Esto puede permitir al atacante ejecutar comandos en la base de datos que no estaban previstos.

>- Abusing boot2docker [Docker Toolbox]

Docker Toolbox es un conjunto de herramientas para ejecutar Docker en sistemas operativos donde Docker no se ejecuta de forma nativa, como versiones antiguas de Windows y macOS. Incluye **boot2docker**, que es una máquina virtual ligera basada en Linux diseñada para ejecutar Docker. Perouna mala gestión de credencials y/o vulimenes la hacer potencialmente explotable

Ethical hacking lab : Toolbox HackTheBox

>- Pivoting

técnica utilizada en pruebas de penetración y hacking ético para acceder a otras partes de una red que inicialmente están fuera del alcance directo. Una vez que un atacante compromete una máquina en la red, puede usarla como un punto de apoyo para atacar otros sistemas en la misma red o en redes adyacentes, ampliando su acceso y comprometiendo más activos.

>- theft SSH Credentials

El **robo de llaves SSH id_rsa** es cuando un atacante obtiene acceso no autorizado a las claves privadas de un usuario, lo que le permite conectarse a servidores remotos sin necesitar una contraseña. Esto compromete gravemente la seguridad del sistema afectado.